Advanced VLAN Technologies

Foreword

- VLAN technologies are widely used on campus networks. Typically, VLANs are used to isolate broadcast domains. Each VLAN belongs to a broadcast domain. During network planning, a gateway needs to be allocated to each broadcast domain. If there are too many VLANs, it is difficult to plan IP addresses and a large number of IP addresses may be wasted.
- In addition, in large enterprises, internal employees as well as many partners work in the enterprise campus. Partners cannot directly access each other. Each partner needs to be assigned a VLAN for isolation, which makes network management and maintenance difficult. Are there any better technologies to solve these problems?
- This course describes several advanced VLAN technologies, including VLAN aggregation, MUX VLAN, and QinQ.

Objectives

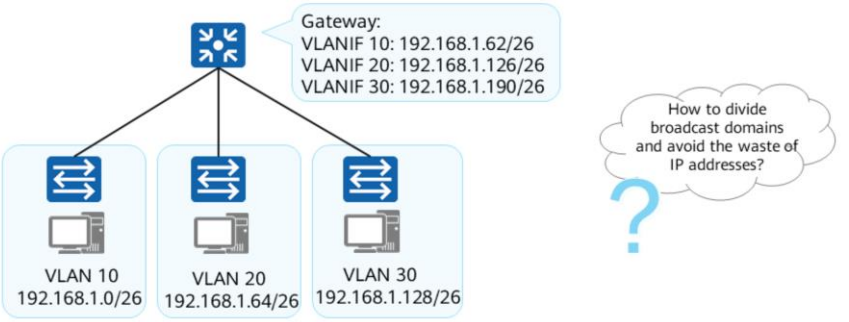
- Upon completion of this course, you will be able to:
  - Describe the working mechanism of VLAN aggregation.
  - Describe application scenarios of MUX VLAN.
  - Describe QinQ implementation.
  - Perform configurations of VLAN aggregation, MUX VLAN, and QinQ.

Contents

HUAWEI

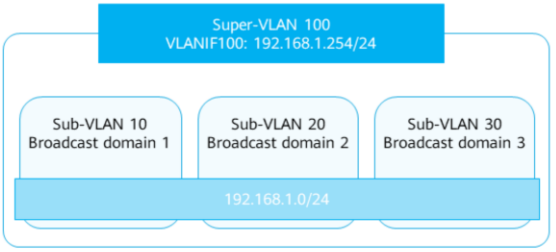
Background of VLAN Aggregation

- Usually, a Layer 3 switch uses a Layer 3 logical interface in each VLAN to allow hosts in different broadcast domains to communicate. This wastes IP addresses.
- On a subnet corresponding to a VLAN, the subnet ID, directed broadcast address, and subnet default gateway address all cannot be used as IP addresses of hosts in the VLAN. In addition, IP addresses available in a subnet may exceed the number of hosts. These excess IP addresses cannot be used by other VLANs.

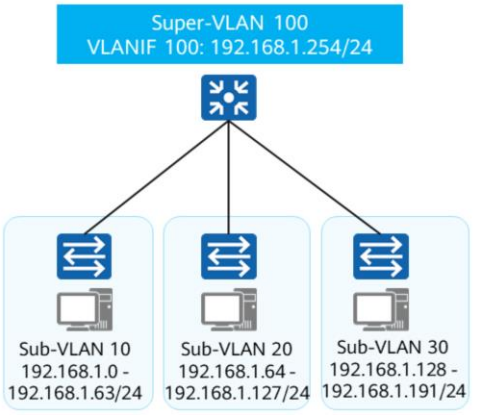


Overview of VLAN Aggregation

- VLAN aggregation, also called super-VLAN, partitions a broadcast domain into multiple VLANs (sub-VLANs) on a physical network and aggregates the sub-VLANs into a single logical VLAN (super-VLAN). The sub-VLANs use the same IP subnet and default gateway address, so the number of IP addresses used is reduced.
- **Sub-VLAN**: contains only physical interfaces, and is used to isolate broadcast domains. A sub-VLAN cannot be used to create a Layer 3 VLANIF interface. Hosts in each sub-VLAN use the VLANIF interface of its super-VLAN to communicate with external devices at Layer 3.
- **Super-VLAN**: A super-VLAN contains only Layer 3 VLANIF interfaces and does not contain physical interfaces. A super-VLAN corresponds to a subnet gateway. Different from a common VLAN, the VLANIF interface status of a super-VLAN depends on the physical interface status of the sub-VLANs in the super-VLAN.



Principle of VLAN Aggregation



The default gateway address of all hosts is 192.168.1.254/24.

VLAN aggregation maps each sub-VLAN to a broadcast domain, associates a super-VLAN with multiple sub-VLANs, and then assigns just one IP subnet to the super-VLAN. This ensures that all sub-VLANs use the IP address of the associated super-VLAN as the gateway IP address to implement Layer 3 connectivity.

- Sub-VLANs share one gateway address to reduce the number of subnet addresses, subnet default gateway addresses, and directed broadcast IP addresses. The switch assigns IP addresses to hosts in sub-VLANs according to the number of hosts. This ensures that each sub-VLAN acts as an independent broadcast domain, conserves IP addresses, and implements flexible addressing.

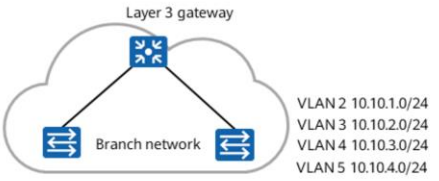
Application of VLAN Aggregation

For traditional VLAN technology, each VLAN needs to be assigned a different IP address segment. In this example, four IP address segments and four routes are required. In super-VLAN mode, only one IP address segment needs to be allocated. Layer 2 VLANs of the super-VLAN share the same IP address segment and Layer 3 gateway. In addition, Layer 2 isolation is implemented between VLANs.

Traditional VLAN assignment

On a branch network, each service is assigned a VLAN, and each VLAN is assigned a network segment.

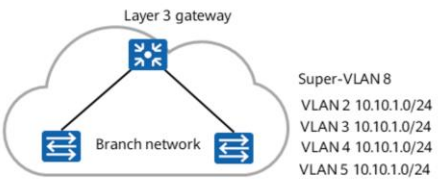
Four VLANs and four gateways



Super-VLAN assignment

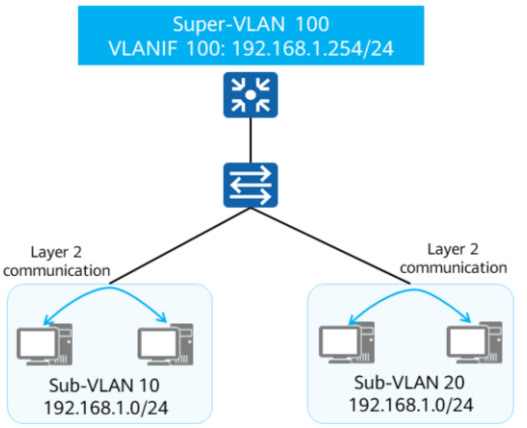
The branch network uses a super-VLAN to aggregate all Layer 2 VLANs. All Layer 2 VLANs share the same IP network segment and are isolated at Layer 2.

Four sub-VLANs, with the IP address of the VLANIF interface of a super-VLAN used as the gateway address

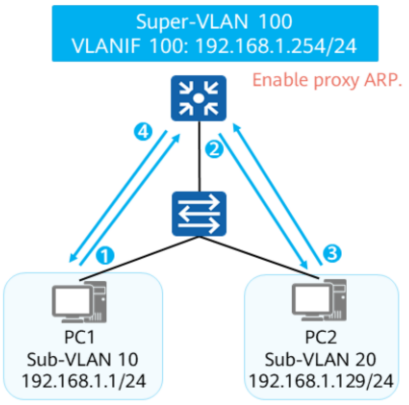


Communication in a Sub-VLAN

A sub-VLAN belongs to a broadcast domain, so devices in the same sub-VLAN can directly communicate with each other at Layer 2.



Communication Between Sub-VLANs

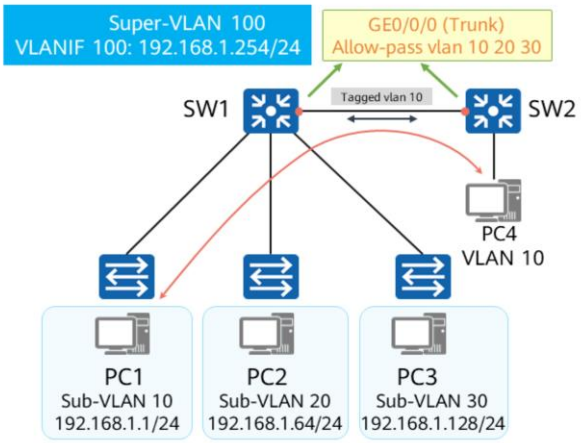


After proxy ARP is enabled on VLANIF 100 of the super-VLAN, communication between PC1 and PC2 is as follows:

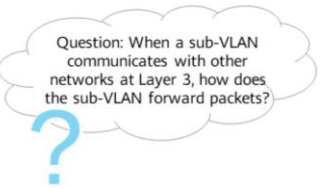
1. When PC1 finds that PC2 is on the same network segment as itself and its ARP table does not contain the entry corresponding to PC2, PC1 broadcasts an ARP Request packet to request the MAC address of PC2.
2. VLANIF 100 corresponding to super-VLAN 100 receives the ARP Request packet from PC1. Because proxy ARP between sub-VLANs is enabled on the gateway, the gateway broadcasts an ARP Request packet to all sub-VLANs of super-VLAN 100 to request the MAC address of PC2.
3. After receiving the ARP Request packet, PC2 returns an ARP Reply packet.
4. After receiving the ARP Reply packet from PC2, the gateway sends its MAC address to PC1. Then PC1 sends the packets destined for PC2 to the gateway, and the gateway forwards the packets at Layer 3.

- When hosts in different sub-VLANs communicate with each other, the hosts send ARP Request packets because IP addresses of the sub-VLANs belong to the same network segment. Actually, different sub-VLANs belong to different broadcast domains. As a result, ARP packets cannot be transmitted to other sub-VLANs, there is no response to ARP Request packets, and the device cannot learn the MAC address of the peer end. As a result, sub-VLANs cannot communicate with each other.
- To implement communication between sub-VLANs, enable proxy ARP on the VLANIF interface of the super-VLAN.

Layer 2 Communication Between Hosts in Sub-VLANs and Other Devices



- Layer 2 communication between hosts in sub-VLANs and other devices is the same as Layer 2 communication within a common VLAN.
- A super-VLAN does not belong to any physical interface. That is, a super-VLAN does not process any packet that carries a super-VLAN tag.



HUAWEI

- An example of Layer 2 communication of a sub-VLAN is as follows:
  - Packets sent from Host_1 to Switch_1 are tagged with VLAN 10. Although sub-VLAN 10 belongs to super-VLAN 100, SW1 does not change VLAN 10 to VLAN 100 in packets.
  - Packets sent from GE0/0/0 on SW1 are still tagged with VLAN 10. SW1 does not send packets from VLAN 100. When another device sends packets from VLAN 100 to SW1, SW1 discards the packets because there is no physical interface corresponding to super-VLAN 100 on SW1.
  - For other devices, only sub-VLANs 10, 20, and 30 are valid and all packets are exchanged in the VLANs. The communication between SW1 configured with VLAN aggregation and other devices is similar to normal Layer 2 communication without the super-VLAN.
- When a PC in a sub-VLAN needs to communicate with other networks at Layer 3, the PC sends data to the default gateway, that is, the VLANIF interface corresponding to the super-VLAN, and then routes the data.

VLAN Aggregation Configuration Commands

1. Create a super-VLAN.

   [Huawei-vlan100] **aggregate-vlan**

   A super-VLAN cannot contain any physical interface, and VLAN 1 cannot be configured as a super-VLAN. The VLAN ID of a super-VLAN must be different from the VLAN ID of a sub-VLAN.

2. Add sub-VLANs to the super-VLAN.

   [Huawei-vlan100] **access-vlan** { *vlan-id1* [**to** *vlan-id2*] }

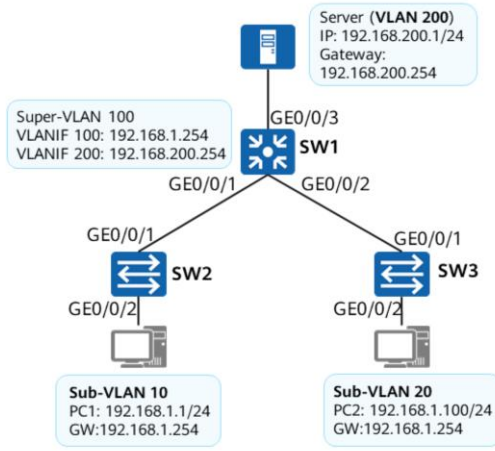
   Before adding any sub-VLANs to a super-VLAN, ensure that they are not configured with VLANIF interfaces.

3. (Optional) Enable proxy ARP on the VLANIF interface corresponding to a super-VLAN.

   [Huawei-vlanif100] **arp-proxy inter-sub-vlan-proxy enable**

   Enable proxy ARP between sub-VLANs.

Example for Configuring VLAN Aggregation (1)

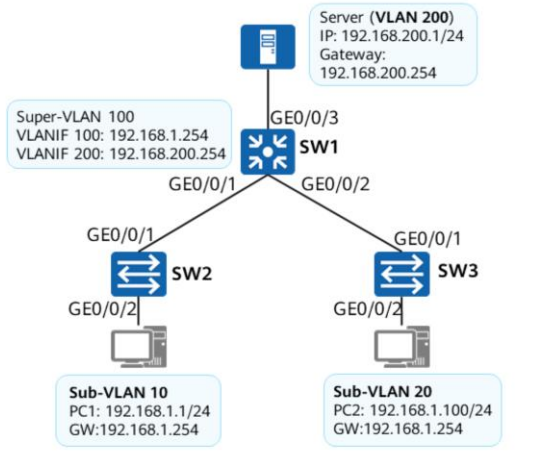


VLAN aggregation is configured on SW1, as shown in the figure.

SW1 configuration:

```
[SW1] vlan batch 10 20    # Create sub-VLANs.
[SW1] interface GigabitEthernet0/0/1
[SW1-GigabitEthernet0/0/1] port link-type trunk
[SW1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SW1] interface GigabitEthernet0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[SW1] vlan 100                # Create a super-VLAN.
[SW1-vlan100] aggregate-vlan
[SW1-vlan100] access-vlan 10 20   #Configure VLAN 10 and VLAN 20 as sub-VLANs of VLAN 100.
[SW1] interface vlanif 100
[SW1-vlanif100] ip address 192.168.1.254 24
[SW1-vlanif100] arp-proxy inter-sub-vlan-proxy enable
# Enable proxy ARP between sub-VLANs.
```

Example for Configuring VLAN Aggregation (2)



VLAN aggregation is configured on SW1, as shown in the figure.

SW1 configuration:

```
[SW1] vlan 200
[SW1] interface GigabitEthernet0/0/3
[SW1-GigabitEthernet0/0/3] port link-type access
[SW1-GigabitEthernet0/0/3] port default vlan 200
[SW1] interface vlanif 200
[SW1-VLANIF200] ip address 192.168.200.254 24
```

SW2 configuration:

```
[SW2] vlan 10
[SW2] interface GigabitEthernet0/0/2
[SW2-GigabitEthernet0/0/2] port link-type access
[SW2-GigabitEthernet0/0/2] port default vlan 10
[SW2] interface GigabitEthernet0/0/1
[SW2-GigabitEthernet0/0/1] port link-type trunk
[SW2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
```

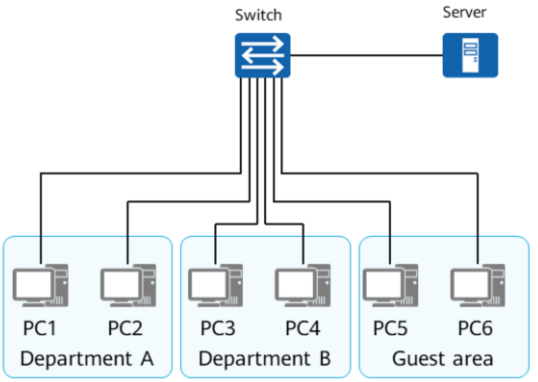
The configuration of SW3 is similar to that of SW2, and is not provided.

Contents

HUAWEI

Background of MUX VLAN

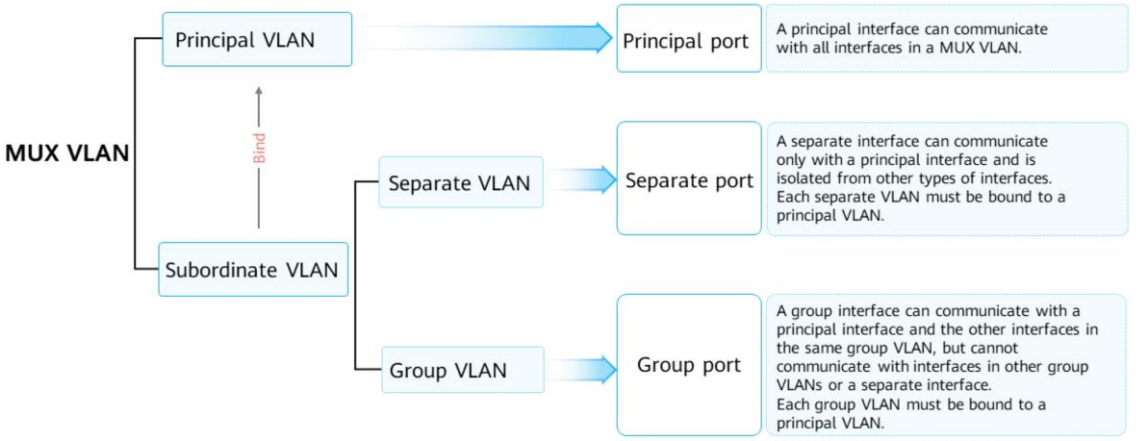
On an enterprise network, networks of different departments need to be independent of each other. VLAN technology can be used to meet this requirement. If a large-scale enterprise has a large number of partners, the partners must be able to access the servers of the enterprise but cannot access each other. In this case, the traditional VLAN technology requires a large number of VLAN IDs and increases the workload of network administrators and maintenance workload.



The Multiple VXLAN (MUX VLAN) function is used to control network resources based on VLANs.

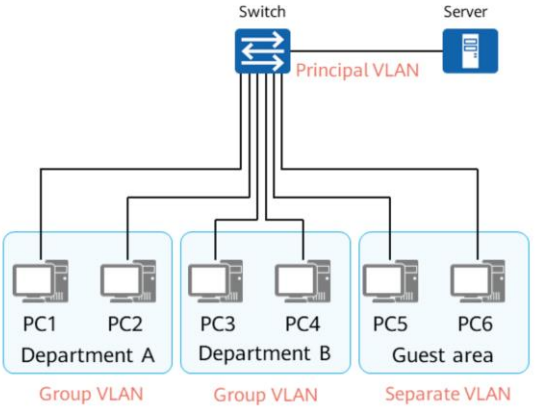
Basic Concepts of MUX VLAN

MUX VLANs are classified into principal VLANs and subordinate VLANs. Subordinate VLANs are classified into separate VLANs and group VLANs.



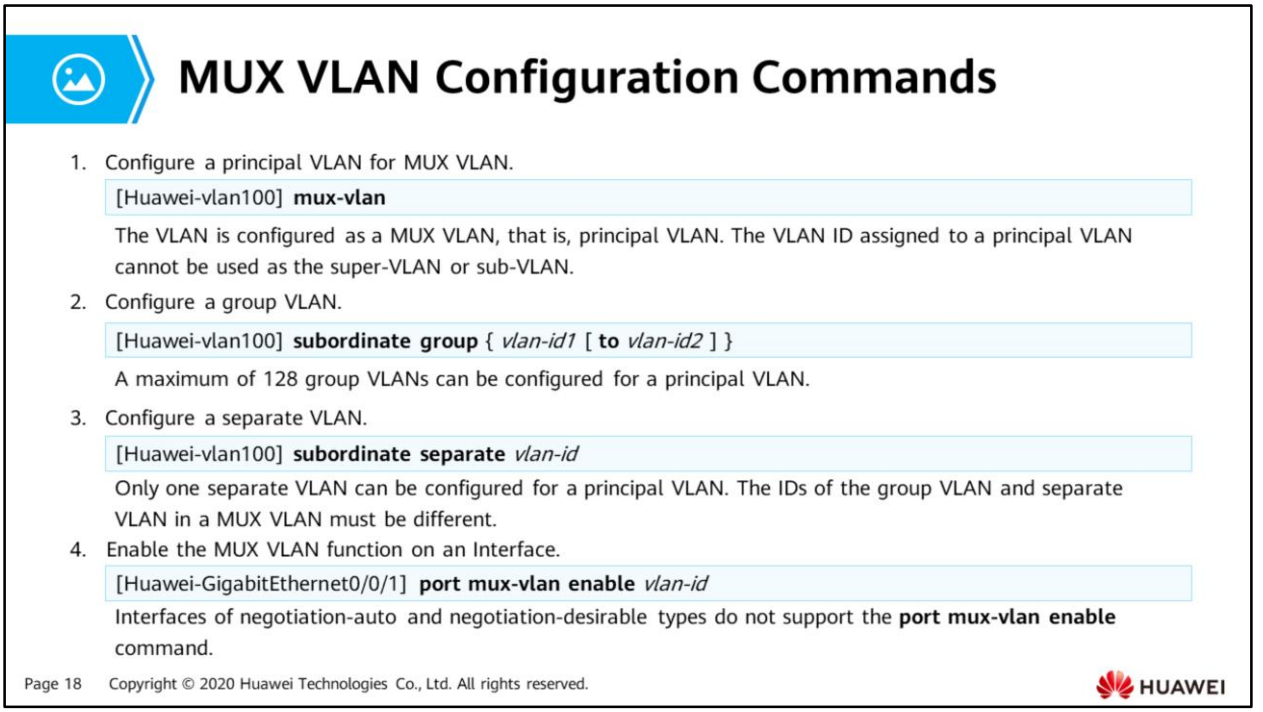
- Either the separate VLAN or group VLAN must be bound to a principle VLAN.
- Interfaces in a principal VLAN can communicate with other interfaces in the same MUX VLAN.

Application of MUX VLAN



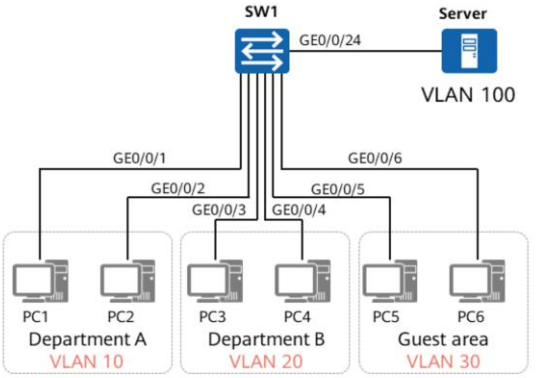
On a switch, VLANs of departments A and B are configured as subordinate group VLANs, the VLAN of the guest area is configured as a subordinate separate VLAN, and the VLAN of the interface connected to the server is configured as the principal VLAN. In addition, all the subordinate VLANs are bound to the principal VLAN. In this way, the following network design requirements are met:

- PCs in department A can communicate with each other at Layer 2.
- PCs in department B can communicate with each other at Layer 2.
- Hosts in departments A and B are isolated at Layer 2.
- Employees in departments A and B can access the server at Layer 2.
- Any PC in the guest area can access only the server and cannot access any other devices, including other guests.



- The MUX VLAN function must be enabled to implement the following functions: The principal VLAN and subordinate VLAN can communicate with each other. Interfaces in a group VLAN can communicate with each other. Interfaces in a separate VLAN cannot communicate with each other.

MUX VLAN Configuration Example



- **Requirements:**
  - The server can communicate with all hosts at Layer 2.
  - Department A, department B, and the guest area cannot communicate with each other at Layer 2.
  - PCs in departments A and B can communicate with each other at Layer 2.
  - Hosts in the guest area cannot communicate with each other at Layer 2.

SW1 configuration:

```
[SW1] vlan batch 10 20 30 100          # Create a VLAN.
[SW1] vlan 100
[SW1-vlan100] mux-vlan
# Specify VLAN 100 as the principal VLAN.
[SW1-vlan100] subordinate group 10 20
# Configure VLAN 10 and VLAN 20 as group VLANs.
[SW1-vlan100] subordinate separate 30
# Configure VLAN 30 as a separate VLAN.
[SW1] interface GigabitEthernet0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
[SW1-GigabitEthernet0/0/1] port mux-vlan enable vlan 10
# Add interfaces to related VLANs and enable the MUX VLAN function.
# The configurations of other interfaces are similar to the configuration of
GE0/0/1, and are not provided.
```

Verifying the MUX VLAN Configuration

Check the VLAN configuration and run the **ping** command to check the network connectivity between PC5 (192.168.1.5/24) and PC6 (192.168.1.6/24).

```
[SW1]display vlan
The total number of vlans is : 5
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
VID  Type    Ports
--------------------------------------------------------------------------------
10   mux-sub UT:GE0/0/1(U)     GE0/0/2(U)
20   mux-sub UT:GE0/0/3(U)     GE0/0/4(U)
30   mux-sub UT:GE0/0/5(U)     GE0/0/6(U)
100  mux     UT:GE0/0/24(U)
```

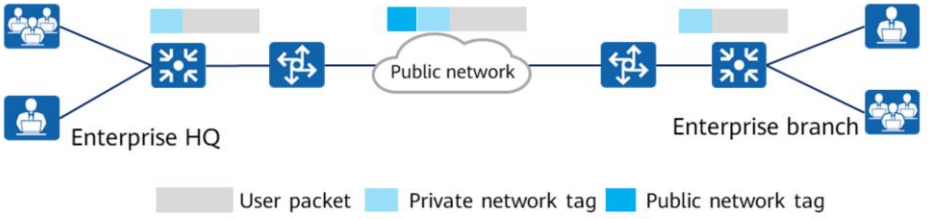
```
PC5>ping 192.168.1.6

Ping 192.168.1.6: 32 data bytes, Press Ctrl_C to break
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable
From 192.168.1.5: Destination host unreachable

--- 192.168.1.6 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

Contents

HUAWEI

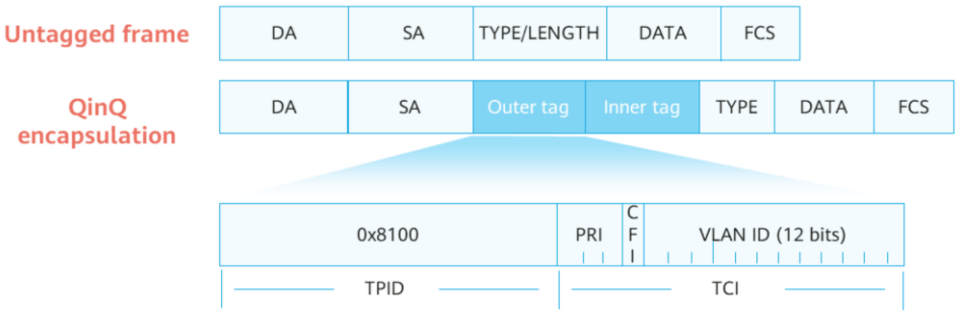
Overview of QinQ

- As Ethernet technologies have been deployed on many networks, using only the VLAN tag defined in IEEE 802.1Q cannot effectively identify and isolate a large number of users. A 12-bit VLAN tag defined in IEEE 802.1Q identifies a maximum of only 4096 VLANs, which is insufficient for a great number of users on the metro Ethernet. 802.1Q-in-802.1Q (QinQ) was developed to expand VLAN space beyond 4096 VLANs.
- QinQ expands VLAN space by adding an additional 802.1Q tag to 802.1Q tagged packets.
- As shown in the figure, user packets carry double tags on the public network. The inner tag is a private network tag, and the outer tag is a public network tag.



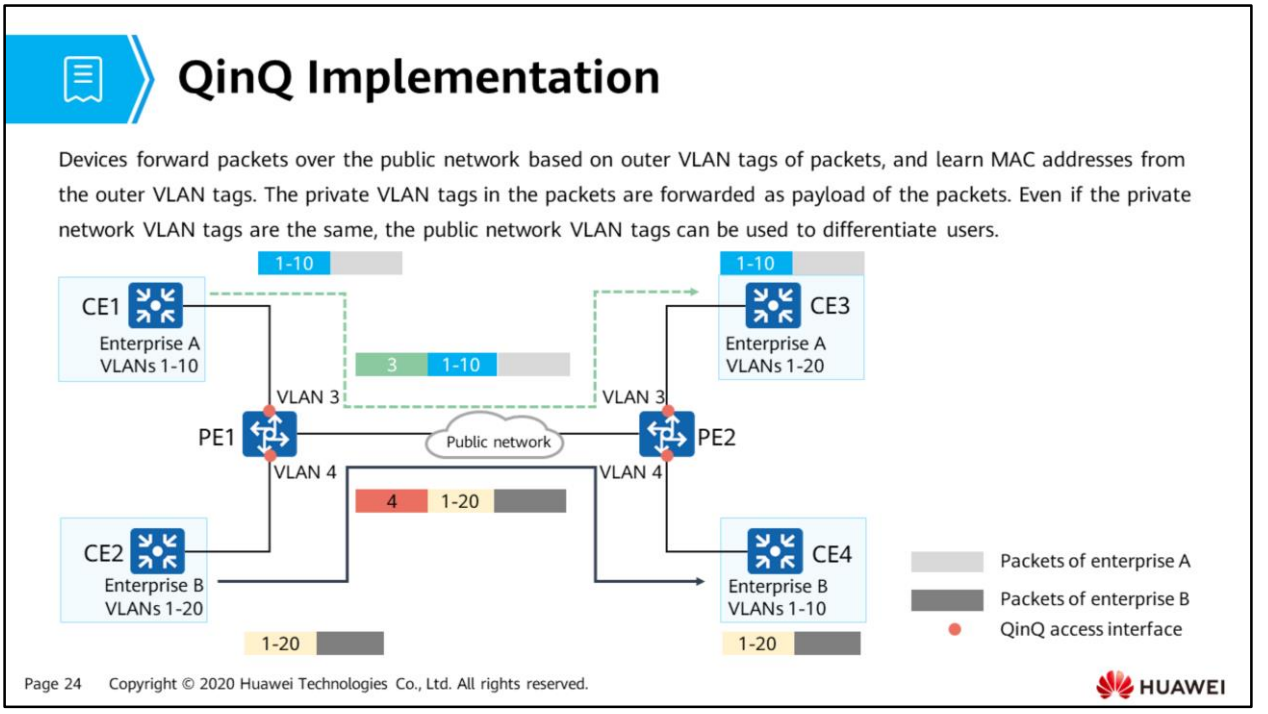
Format of QinQ Packets

In QinQ encapsulation, two VLAN tags are added to the end of the source MAC address field of an untagged Ethernet data frame.



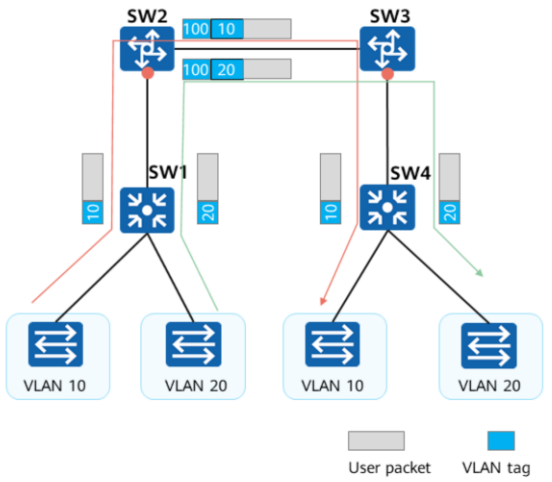
HUAWEI

- Tag Protocol Identifier (TPID): indicates the frame type. The value 0x8100 indicates an 802.1Q-tagged frame. A device that does not support 802.1Q discards 802.1Q frames.
- For the inner 802.1Q tag, the value is set to 0x8100. For the outer 802.1Q tag, different vendors may use different values.
  - 0x8100: is used by Huawei routers.
  - 0x88A8: 802.1ad specifies that the TPID in the outer 802.1Q tag is 0x88a8.
- On a Huawei device, the default value of the outer 802.1Q tag is 0x8100, which can be changed using a command.



- The private VLANs of enterprise A and enterprise B are VLANs 1 to 10 and VLANs 1 to 20, respectively. The public network allocates public VLANs 3 and 4 to enterprise A and enterprise B respectively. When tagged packets from enterprises A and B arrive at the public network, they are tagged with additional VLAN tags, that is, VLAN 3 for enterprise A's packets and VLAN 4 for enterprise B's packets. In this way, packets from enterprise networks are separately transmitted on the public network, even though the two networks have overlapping VLAN IDs. After packets traverse the public network, public VLAN tags of the packets at the receiving PE are removed. Then the packets are forwarded to the CE of their respective user network.

Implementation of QinQ — Basic QinQ



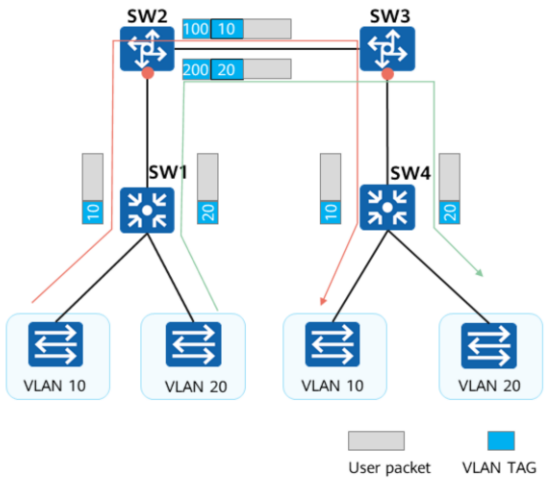
Packet processing of basic QinQ:

1. SW1 receives a packet tagged with VLAN 10 or 20 and sends the packet to SW2.
2. When receiving the packet, SW2 adds an outer tag with VLAN 100 to the packet.
3. The packet with double tags is forwarded according to the Layer 2 forwarding process.
4. After receiving the packet from VLAN 100, SW3 removes the outer tag with VLAN 100. SW3 then sends the packet that carries only one tag with VLAN 10 or 20 to SW4.
5. After receiving the packet, SW4 forwards it according to its VLAN ID and destination MAC address.

HUAWEI

- Basic QinQ is implemented based on interfaces. When a packet arrives at an interface that has basic QinQ enabled, the device will tag it with the interface's default VLAN tag, regardless of whether the packet is already tagged or untagged. After being processed by basic QinQ on an interface, single-tagged packets change into double-tagged packets, and untagged packets change into single-tagged packets with the default VLAN tag of the interface.
- Interface-based QinQ inflexibly encapsulates the outer VLAN tag. The device on which interface-based QinQ is enabled cannot change the encapsulation method used for the outer VLAN tag based on service types.

Implementation of QinQ — Selective QinQ



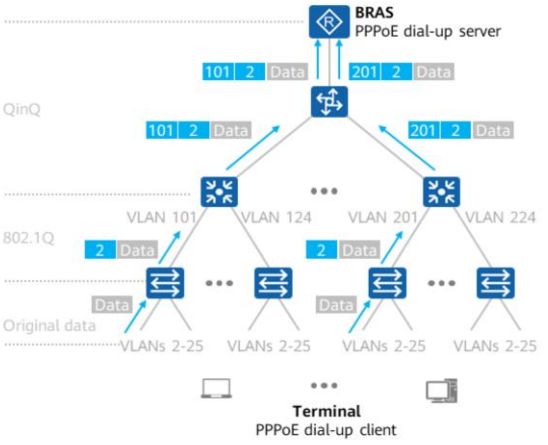
Packet processing of selective QinQ:

1. When receiving the packet tagged with VLAN 10 or VLAN 20, SW1 forwards the packet to SW2.
2. When receiving the packet tagged with VLAN 10, SW2 adds an outer tag with VLAN 100 to the packet. When receiving the packet tagged with VLAN 20, SW2 adds an outer tag with VLAN 200 to the packet.
3. The packet with double tags is forwarded according to the Layer 2 forwarding process.
4. After receiving the packet, SW3 removes the outer tag with VLAN 100 or 200. SW3 then sends the packet that carries only one tag with VLAN 10 or 20 to SW4.
5. After receiving the packet, SW4 forwards it according to its VLAN ID and destination MAC address.

HUAWEI

- Selective QinQ allows the device to select whether to tag packets, or determine the type of outer VLAN tags to be encapsulated, according to the traffic classification result. Selective QinQ can classify traffic based on the VLAN tag, priority, MAC address, IP protocol, source IP address, destination IP address, or port number of an application program.
- VLAN ID-based selective QinQ: adds outer VLAN tags based on inner VLAN IDs.
- 802.1p priority-based selective QinQ: adds outer VLAN tags based on 802.1p priorities in inner VLAN tags.
- Traffic policy-based selective QinQ: adds different outer VLAN tags based on QoS policies so that differentiated services can be provided based on service types.
- Selective QinQ is an extension of basic QinQ and is more flexible. The difference is as follows:
  - Basic QinQ: adds the same outer VLAN tag to all packets arriving at a Layer 2 interface.
  - Selective QinQ: adds different outer VLAN tags to packets arriving at a Layer 2 interface based on inner VLAN tags.

QinQ Application on Campus Networks



Scenario Requirements:

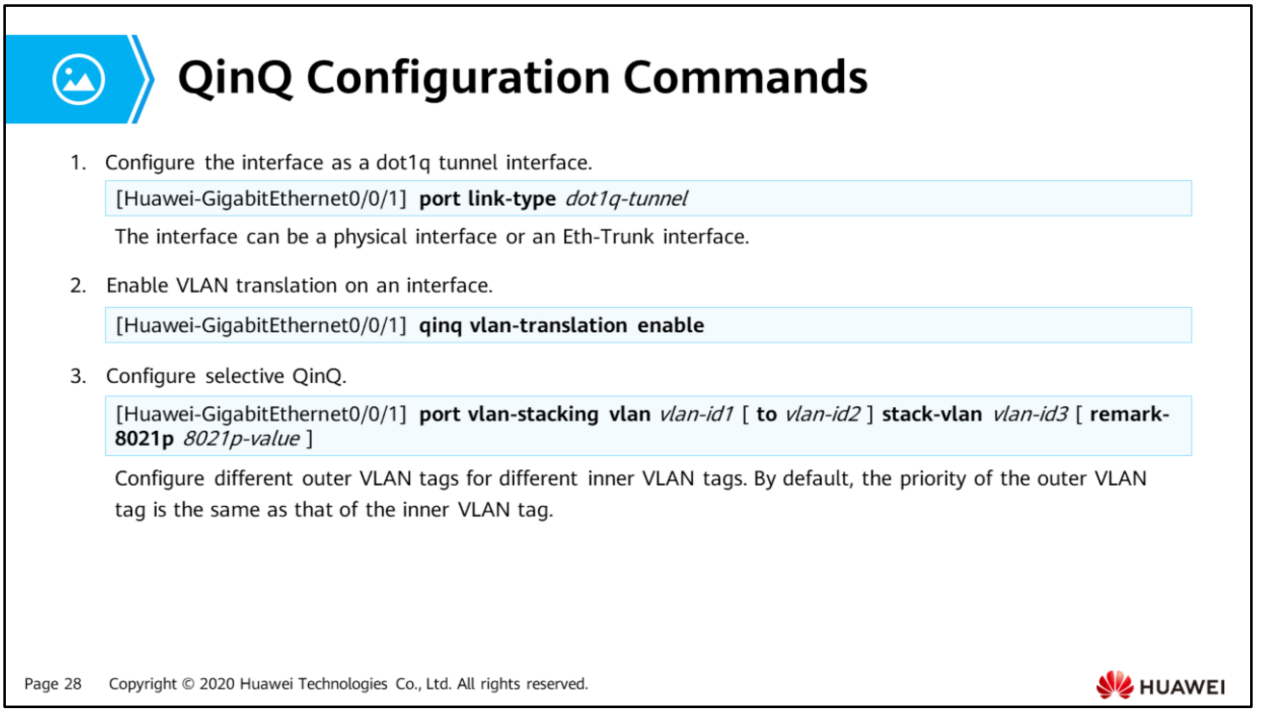
1. A single terminal user can be traced.
2. Each terminal is assigned to an independent Layer 2 broadcast domain, minimizing the impact of BUM traffic on the network.
3. Terminals can communicate with the BRAS at Layer 2 to meet PPPoE authentication requirements.

Solution

1. The access switch assigns an independent VLAN for each downlink interface.
2. The access switch adds an 802.1Q tag to the original data before forwarding the data to the aggregation switch.
3. QinQ is deployed on the aggregation switch. Each downlink interface is assigned an independent VLAN (each access switch corresponds to a unique VLAN). The aggregation switch adds a Layer 2 tag to the traffic and sends the traffic to the core switch.
4. The core switch transparently transmits the traffic to the BRAS, and the BRAS performs QinQ decapsulation.

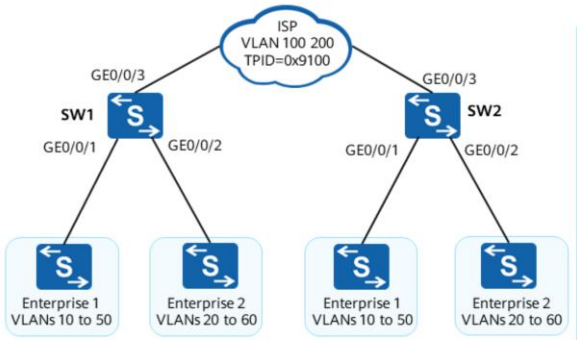
HUAWEI

- Broadband Remote Access Server (BRAS): The BRAS aggregates and forwards service flows, meeting different user requirements for the transmission rate and broadband utilization. Therefore, it is the core device for broadband user access.
- Broadcast, unknown unicast, and multicast (BUM): The switch floods BUM packets.



- Selective QinQ must be configured on the hybrid interface and the **qinq vlan-translation enable** command must have been executed to enable VLAN translation. Selective QinQ can only take effect on the interface in the inbound direction.
- When an interface configured with VLAN stacking needs to remove the outer tag from outgoing frames, the interface must join the VLAN specified by **stack-vlan** in untagged mode. If the outer VLAN does not need to be removed, the interface must join the VLAN specified by **stack-vlan** in tagged mode.

Example for Configuring Basic QinQ



Requirements:

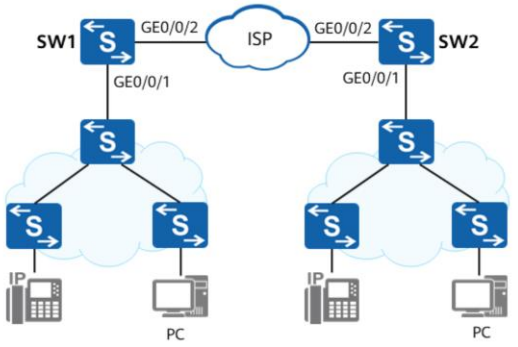
- Enterprise 1 and enterprise 2 are connected to the same ISP network and use the same VLAN space.
- The ISP uses QinQ technology to implement data exchange between different sites of the same enterprise.
- VLAN 100 and VLAN 200 are planned for enterprise 1 and enterprise 2, respectively.

SW1 configuration:

```
[SW1] vlan batch 100 200
[SW1] interface GigabitEthernet 0/0/1
# Configure VLAN 100 as the default VLAN on GE0/0/1.
[SW1-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[SW1 -GigabitEthernet0/0/1] port default vlan 100
[SW1] interface GigabitEthernet 0/0/2
# Configure VLAN 200 as the default VLAN on GE0/0/2.
[SW1-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[SW1-GigabitEthernet0/0/2] port default vlan 200
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200
# Set the TPID value in the outer VLAN tag.
[SW1-GigabitEthernet0/0/3] qinq protocol 9100
```

The configuration of SW2 is similar to that of SW1, and is not provided.

Example for Configuring Selective QinQ



Requirements:

- Internet access users and VoIP users access the ISP network through SW1 and SW2 and communicate with each other through the ISP network. The enterprise assigns VLAN 100 to PCs and VLAN 300 to VoIP phones.
- Packets from PCs and VoIP terminals need to be transmitted over the ISP network in VLAN 2 and VLAN 3 respectively.

SW1 configuration:

```
[SW1] vlan batch 2 3
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid untagged vlan 2 3
[SW1-GigabitEthernet0/0/1] qinq vlan-translation enable
[SW1-GigabitEthernet0/0/1] port vlan-stacking vlan 100 stack-vlan 2
[SW1-GigabitEthernet0/0/1] port vlan-stacking vlan 300 stack-vlan 3
[SW1-GigabitEthernet0/0/1] quit
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 3
[SW1-GigabitEthernet0/0/2] quit
```

The configuration of SW2 is similar to that of SW1, and is not provided.

Quiz

1. (Single) When a sub-VLAN communicates with an external network at Layer 2, what is the VLAN tagged to packets on the outbound interface?
   A. Sub-VLAN
   B. Secondary VLAN
   C. Super-VLAN
   D. Isolate VLAN
2. (Single) Which of the following statements about QinQ is false?
   A. QinQ packets are forwarded based on outer VLAN tags on the public network.
   B. QinQ packets are forwarded based on inner VLAN tags on the public network.
   C. QinQ provides a simpler Layer 2 VPN tunneling technology.
   D. QinQ can be realized through static configuration, without a signaling protocol.

1. A
2. B

Summary

- To implement VLAN aggregation, you need to configure a super-VLAN and sub-VLANs. To enable communication between different sub-VLANs, you need to enable proxy ARP in the super-VLAN. VLAN aggregation prevents complex network address planning caused by subnet assignment and isolates broadcast domains through VLANs.
- The MUX VLAN includes a principal VLAN and subordinate VLANs. Subordinate VLANs are classified into separate and group VLANs. A separate interface can communicate only with a principal interface and is isolated from other types of interfaces. A group interface can communicate with a principal interface and the other interfaces in the same group VLAN, but cannot communicate with interfaces in other group VLANs or a separate interface.
- QinQ technology expands the number of VLANs, and allows user packets tagged with private VLAN IDs to be transparently transmitted on the public network.


Thank You
www.huawei.com